

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
16 September 2021 (16.09.2021)



(10) International Publication Number
WO 2021/180812 A1

(51) International Patent Classification:

G06F 21/54 (2013.01) G06F 21/78 (2013.01)
G06F 9/455 (2018.01)

(21) International Application Number:

PCT/EP2021/056100

(22) International Filing Date:

10 March 2021 (10.03.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/816,467 12 March 2020 (12.03.2020) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York, 10504 (US).

(71) Applicant (for MG only): **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB).

(72) Inventors: **GREEN, Matthew**; IBM AUSTRALIA LIMITED, LEVEL 4, 1 CORPORATE COURT, BUNDALL, Queensland 4217 (AU). **MADINENI, Narayana, Aditya**; IBM AUSTRALIA LIMITED, LEVEL 4, 1 CORPORATE COURT, BUNDALL, Queensland 4217 (AU).

GRAY, Michael; IBM AUSTRALIA LIMITED, LEVEL 4, 1 CORPORATE COURT, BUNDALL, Queensland 4217 (AU). **MCLEAN, Leigh**; IBM AUSTRALIA LIMITED, LEVEL 4, 1 CORPORATE COURT, BUNDALL, Queensland 4217 (AU).

(74) Agent: **PYECROFT, Justine**; IBM UNITED KINGDOM LIMITED, INTELLECTUAL PROPERTY LAW, HURSLEY PARK, HURSLEY, WINCHESTER Hampshire SO21 2JN (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: VIRTUAL MACHINE PERFECT FORWARD SECRECY

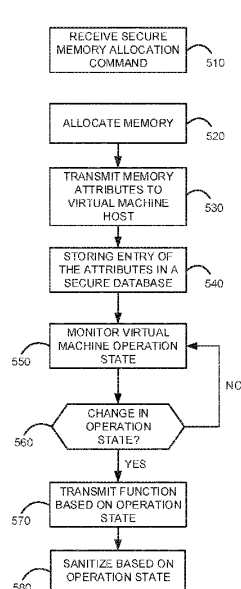


FIG. 5

(57) Abstract: Provided is a method, a computer program product, and a system for providing perfect forward secrecy in virtual machines. The method includes receiving a secure memory allocation function from an application, including a connection secret to be stored in memory. The method further includes allocating memory for the connection secret according to the memory size parameter and storing an entry relating to the connection secret in a secure database. The memory information includes a memory location and a memory size of the memory. The method also includes monitoring an operation state relating to the virtual machine. The method further includes receiving, from the application, a secure deallocation function relating to the connection secret and retrieving the memory information from the secure database. The method also includes deleting the connection from the memory and sanitizing the memory location logged by the memory information.

WO 2021/180812 A1

[Continued on next page]

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*